[19]中华人民共和国专利局

[11] 公开号 CN 1118482A

[12] 发明专利申请公开说明书

[21]申请号 95108181.0

[51]Int.Cl[6]
G06F 17/60

[43]公开日 1996 年 3 月 13 日

[22]申请日 95.6.29

[30]优先权

[32]94.6.30 [33]US[31]269,205

[71]申请人 坦德姆计算机公司

地址 美国加利福尼亚

[72]发明人 W·戴尔·霍普金斯

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

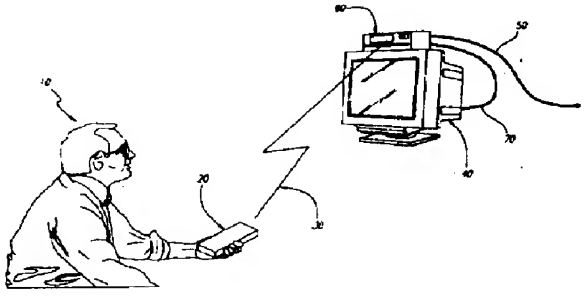
代理人 杜日新

权利要求书 5 页 说明书 13 页 附图页数 6 页

[54]发明名称 远程金融业务系统

[57]摘要

这是一个处理远程金融业务的系统，该系统采用具有存储器、并经交互网络与异地处理系统进行通信联络的付账模块，付账模块将付款账户信息和相应的 PIN 信息存入存储器中。用户可以选择一种金融业务和一个付款账户来进行该金融业务。PIN 和所需的付款账户信息可以从存储器中获取，这些信息经过加密、经由交互网络最终转输给管理账户的金融机构，金融机构可作出接受／拒绝的决定，并经交互网络将接受／拒绝信息传送给用户。



权 利 要 求 书

1. 一种利用与异地处理系统进行通信联络的付账模块进行远程金融业务的方法，其中，付账模块寻访存储数据存储器，识别至少一种付款账户和至少一种密码口令，本方法包括：

由付账模块向异地处理系统提供识别付款账户的信息，其中识别付款账户的信息是依据存储器中存储的数据；和

由付账模块向异地处理系统提供密码口令。

2. 权利要求 1 的方法，还包括，在提供付账账户识别信息之前，初始化付账模块的步骤，其中初始化步骤对每个所需付款账户只需进行一次该初始化步骤包括以下步骤：

将识别至少一个付款账户的信息存储到存储器中；

存储器中至少存储一种密码口令，其中在付账模块中储存有识别信息的每一账户，至少有一相应的存储密码口令。

3. 权利要求 2 的方法，还包括：在存储器中存储一种存取密码口令。

4. 权利要求 2 的方法，还包括：在提供加密口令步骤之前，对提供加密口令步骤中所提供的加密口令进行加密。

5. 权利要求 4 的方法，其加密步骤采用每项业务活动导出唯一密钥技术进行。

6. 权利要求 1 的方法，还包括：在提供进行识别付款账户信息这一步骤之前，对该识别付款账户信息进行加密。

7. 权利要求 6 的方法，其中给识别付款账户信息加密的步骤，采用每项业务活动导出唯一密钥技术来进行。

8. 权利要求 1 的方法，还包括：在提供识别付款账户信息这一步骤之前：

把存取密码输入付账模块，其中，进行远程金融业务活动之前必须输入正确的存取密码口令；并

确认是否输入了正确的存取密码口令。

9. 权利要求 1 的方法，还包括选择付款账户的步骤，其中

提供识别付款账户信息的步骤包括提供在选择步骤中所选识别付款账户的信息；

提供密码口令的步骤包括提供与在选择步骤中所选择的付款账户相对应的密码口令。

10. 权利要求 1 的方法，还包括：在提供信息的步骤之前，给用户提供金融业务选择的步骤。

11. 权利要求 10 的方法，包括：在给用户提供金融业务选择的步骤之后，选择金融业务的步骤。

12. 权利要求 1 的方法，还包括：从异地处理系统给付账模块发送接受/拒绝信息的步骤。

13. 权利要求 1 的方法，其中提供信息的步骤包括将识别付款账户信息提供到有线电视传输系统。

14. 权利要求 1 的方法，其中提供信息的步骤包括：向 *ATM* 网络提供识别付款账户的信息。

15. 权利要求 9 的方法，其中选择付款账户的步骤包括：

提供一个在显示屏显示付款账户目录的图表；并且

从显示的所列付款账户中选择一个付款账户。

16. 权利要求 15 的方法，其中选择付款账户步骤包括：使用输入设备在屏幕上移动指示标记到欲选付款账户的相应位置。

17. 权利要求 1 的方法，还包括：

在显示设备上显示菜单和提示；

使用菜单和提示处理远程金融业务。

18. 权利要求 1 的方法，还包括：

由异地处理系统决定是否接受/拒绝金融业务。

19. 权利要求 1 的方法，还包括：

在提供识别付款账户信息的步骤之前选择付款账户的步骤。

20. 权利要求 1 的方法，其中加密口令是基于在存储器中存储的识别至少一个密码口令的数据。

21. 权利要求 1 的方法，其中识别至少一个付款账户的数据包括与账户管理机构中至少一个付款账户相对应的数据，还包括：

账户管理机构的授权，允许使用付款账户。

22. 一种远程金融业务设备的初始化方法，该设备包括可存取存有数据的存储器的付账模块，该方法包括：

存储器中存储识别至少一个付款账户的信息；

加密至少一个口令，产生至少一个加密口令，其中在付账模块中存有识别信息的每个付款账户至少有一对应的口令；

在存储器中存储该至少一个加密口令。

23. 权利要求 22 中的初始化方法，其中执行加密步骤，使用至少一个文件加密器。

24. 权利要求 22 中的初始化方法，其中，识别至少一个付款

账户的信息包括与账户管理机构中至少一个付款账户相对应的数据，该方法还包括：

账户管理机构授权，在使用付账模块进行金融业务中，允许使用的付款账户。

25. 执行远程金融业务的设备，具有与异地处理系统的通信联系，该设备包括：

进行金融业务的付账模块，其中付账模块能够与异地处理系统进行通信联络；

一个可由付账模块存取的存储器，存储至少识别一个付账账户和至少一个口令的识别数据。

26. 权利要求 25 的设备，还包括：一个携带数据的交互网络，其中付账模块和交互网络相互通信，传送、接收数据，以及异地处理系统用该交互网络从付账模块接收数据，并向其发送数据。

27. 权利要求 25 的设备，其中，存储器是付账模块的组成部分。

28. 权利要求 26 的设备，其中，付账模块包括：

向异地处理系统提供识别付款账户信息的装置，其中，识别付款账户的信息是基于存储在存储器中的数据；以及

给异地处理系统提供一个加密口令的装置。

29. 权利要求 26 的设备，还包括为加密口令加密的装置。

30. 权利要求 29 的设备，其中，加密装置采用每项业务导出唯一的密钥技术。

31. 权利要求 25 的设备，还包括：把存取口令输入到付账模块的装置，在这里，正确的操作密码必须在进行远程金融业务前输

入；以及

确定输入的操作密码是否正确的装置。

32. 权利要求 28 的设备，还包括选择付款账户的装置，以及其中

提供识别付款账户信息的装置包括：提供识别的选择装置所选定的付款账户信息的装置；并且

提供加密口令的装置包括：提供与选择装置所选定的付款账户相对应的加密口令的装置。

33. 权利要求 28 的设备，还包括为用户提供一个选择金融业务的装置。

34. 权利要求 26 的设备，其中交互网络包括有线电视传输系统。

35. 权利要求 26 的设备，其中交互网络包括 *ATM* 网络。

36. 权利要求 26 的设备，其中交互网络包括 *EFT—POS* 网络。

37. 权利要求 25 的设备，还包括：

响应付账模块所提供的指令的显示屏。

38. 权利要求 37 中的付账模块还包括：

输入装置；以及

使用输入装置来移动显示屏上显示的指示标记的装置。

说　　明　　书

远程金融业务系统

本发明涉及由远处保护和处理金融业务的方法和装置，其中，在远地点和异地业务记录成处理地点之间有通信联络。

为保证遥控进行的金融业务的安全和保密，采用了多种技术，这样的技术通常依靠使用密码，代表性的做法是用“身份标示码”即*PINs*。业务中，*PIN*一般同由阅读器进行扫描的第二种形式的身份证明一起使用。

已知的远程金融业务技术是银行自动出纳机(“*ATMs*”)和销售点电子资金转账机终端(“*EFT—POS*”终端)。典型的*ATMs*和*FT—POS*终端要求用户插入一张编有密码磁条的卡片，读出的信息包括用户姓名、账号、卡有效价值(“*CVV*”)和截止日期。此外还要求用户输入*PIN*，以便开始任何业务。*PIN*由注册机构如银行或信用卡公司指定，用户也可以自行选择自己的*PIN*，在自行选择系统中，用户可以亲往注册机构进行选择。自动出纳机一般离用户家较远。

对*ATM*和*EFT—POS*的网络是众所周知的，这样的一个网络是用*ANSI X*9.24标准进行描述的，该网络中，不同金融机构的*ATM*(或*EFT—POS*)通过中央处理机构相互连接，例如，在某个特定银行有账户的用户，可使用该网络进行金融业务，如从不同的银行提款。该网络广为人知，获得了象“*NYCE*”“*PLUS*”和“*CIRRUS*”

这样的行业名称。典型的网络中 *ATMs* 与银行的数据处理器连接，其它银行再与有类似的 *ATM* 连接。网络中每家银行的数据处理器依次与中央处理机构联网，中央处理机构从而充当起收发员(*router*)或金融网络开关，向网络中相应银行传递业务信息。

ATM 系统一直遭受各种形式的恶意破坏，例如，因用户须自己把 *PINs* 用非密码形式输入系统，*PINs* 是易于接触的，虽然 *ATM* 网络终端在传送 *PINs* 前把它们译成密码，但众多 *PINs* 通常只使用一种加密钥，因此可以用已知的一个 *PIN* 作为破坏基础，使系统容易受到字典式破坏。当已知加密的 *PIN* 被窃听时(如窃听有关未加密账户的资料)，或者当同一个 *PIN* 被窃听时(相应不同账户)，那么因用相同的密码，即可知道该账户的 *PIN*。

已有多种技术解决从远地点选择并加密 *PIN*，用户不需去登记机构。美国专利 4,870,683 号和 4,885,779 号中描述了一种文件加密系统，用户可使用这种文件加密系统在家里选择并加密 *PIN*，然后把它寄给登记机构。用户也可以通过电话线路把加密 *PIN* 传送给登记机构。在远地点选择、加密 *PIN* 的另一种已知技术是，用户使用电子方式与加密系统进行通信联络(例如使用调制解调器通信)，发送标识符、收回加密标识符。这系统在共同转让的未决美国专利申请 08/029,833 号中有描述。

大家知道的还有多种无保安的在家购物系统，在家购物电视就是这样的系统。典型的在家购物系统包括 *QVC* 网络和在家购物频道。在家购物电视系统中，播送的节目通过电视机接收，节目包括出售物品的描述、录像展示、价格和定购指南。典型的做法是提供用户一个用于电话定购的免费电话号码，如“800”，用户可使用信用卡定

购，但要把各种资料交给承接定单的人。这种系统是无保安的，因为电话线路容易受到监听或偷听者的恶意破坏，信用卡资料没有加密，因而破坏者可以通过电话线或者利用接收定单获取有关资料。

其它种类的电视购物所提供的服务是通过电视机进行的无保安、相互影响的定购服务。这种服务通常在饭店使用，在房间里遥控结账。室内电视机向顾客提供各种结账选择，例如可提供给顾客选择复核房费、每天、每顿餐费、电话费等，自动结账，顾客不必到饭店大厅的 登记服务台去。所提供的选择以菜单形式在电视屏蔽上显示，用户使用遥控器如标准的电视手持红外遥控器，使菜单内容上下滚动而进行选择，也可以用遥控器选择不同的菜单。这种系统不能通过电视直接付款，饭店通常收预付款，比如在前台入住登记处提交信用卡（可增加身份证）。但是，通过电话系统窃听电话信号或窃取饭店里顾客信用卡的记录情况，都很容易使该系统遭到恶意破坏。

另一种交互型电视购物系统用于预定或限制使用付费选看的节目。饭店给客户提供的这种付费选看节目服务，允许顾客选择各种电影节目（费用加在饭店账单上），也可选择关掉某些影片或者所有付费选看节目。至于结账系统，用户可以使用标准的手持电视或录像机遥控器上下滚动菜单作出选择，但用户还是不可能直接付账，这些费用加到了饭店或者电话账单上。这种节目选择系统和结账系统一样，也容易遭到恶意的破坏。

计算机公告牌提供了另一种在家购物系统。在俄亥俄州 43220、哥伦布 20212 邮政信箱、阿灵顿中央大道 5000 号的计算机服务部就是这种方式，这样的系统中，用户用个人计算机与远程计算机系统进行联络，用调制解调器来启动远程计算机和公告牌系统之间的电

话联络。用户可以自由浏览所提供的各种服务和出售的物品，用信用卡或者邮寄支票付账。这样的系统容易遭到以下的破坏：电话窃听、监听，与公告牌计算机直接联接监听器等，其它的如对计算机或通过邮政进行破坏等等。

本发明的很大程度上减轻了已有技术和装置中存在的风险和不足，采用密码保安措施以一种选择、执行个人密码的保安方法，提供了一种安全的远程金融业务的系统。本发明提供一种使用付账模块如初始化的遥控设备，通过交互网络，进行远程金融业务的装置和方法。

特别是付账模块同与交互网络相连的接收装置进行联系，诸如与电缆系统连接的电视，以便于进行购物或服务等方面的财务业务。其它具体例子中，付账模块与控制装置分离。

在最佳实施例中，程序设计者通过广播或有线电视提供出售的商品和服务，或通过已有的其它交互传输方式提供，比如卫星传输或电话计算机联络。用户可以观看节目单，使用控制装置自由选择商品或服务，如果希望购物或进行金融业务活动，则可以在屏幕上向人的展示们图像中进行自由选择，就象菜单一样。如果用户只想进行购物业务，则可以在展示的图像中作出相应的选择，这时要求用户把一个密码(这里相当于"*PIN*")输入控制装置，*PIN* 输入后启动了付账模块，接着用户就能选择一种付款方式，如各种预先初始化的信用卡中的任一种。

加密的 *PIN* 存储在付账模块中，它与未加密的 *PIN* 相对应。付账模块采用每个交易导出唯一密钥技术("*DUKPT*"技术)，在 *ANSI*×9.24 标准中举例陈述过，在把已加密 *PIN* 传送给网络之

前，最好给它加密。

然后付账模块把加密 *PIN*（或双重加密 *PIN*）和相关数据（如信用卡或信用卡磁道 1、磁道 2 数据）一起传送给交互网络，网络主机系统再把这个信息传送给相应的金融机构如有关银行。该业务通过金融网传递给发卡者来解密密码信息，并决定是接受还是拒绝该项业务；接受/拒绝信息传回用户那里，相应的接受/拒绝信号在用户显示屏上出现。

在最佳实施例中，付账模块用 *DUKDT* 密钥被初始化，有关所需信用卡和借方卡的识别资料也输入了付账模块，资料由用户以数字序列形式输入付账模块。每张申请信用卡每次都要经过上述步骤，用户监视器上显示提示和指令。用户也可以先输入每张卡的 *PIN* 加密版本。上述文件加密系统可以用来加密 *PIN*。密钥没有保存在付账模块中。

也可要求用户选择用于控制存取付账模块的存取密码，多个用户可以使用同一个付账模块，每个付账模块上都有控制存取该用户自己的卡的个人存取密码。

采用本发明，不用磁条阅读器就能够进行安全的业务活动，并可满足诸如 *ATM* 网络等现有系统的要求，同时付账模块比磁条阅读器更简单，因为它不需要阅读磁条用的装置。

由于不使用不加密 *PIN*，无论是付账模块还是交互网络，都具有比通常的 *ATM* 网络成零售点的销售终端更好的可靠性。这种 *PINs* 在付账模块中以加密方式存储，在不加密方式时传输不到网络中去；解密钥（“*Keys*”）不再保存在付账模块中，更确切地说，这个解密钥只保存在卡片发行人手里而不在网络的其它部分中。

另外，使用了特殊的密钥(如用 *DUKPT* 技术和文件加密器)，防止了恶意的破坏，包括字典式破坏。

本系统的付账模块和现有的 *ATM* 及销售网络终端是全兼容的，这样使用加密和密码保护措施后得到了如上所述的安全性能。

此外，本发明的业务系统给个别银行(和其它付账账户管理机构)以自主处理权，以确定远程金融业务使用的个别银行提供的账户是否符合使用条件。

还有，本发明的设备要比现有的远程处理设备可靠和便宜，例如它省去了磁条阅读器和显示屏(不是用户显示器)占去的空间和费用。

对附图作简要的介绍。

基于上述情况，下面将详细介绍本发明的其它目的和优势，附图的参照号前后是一致的，其中：

图 1 是本发明之远程金融业务系统的地方系统；

图 2 是本发明之远程金融业务系统框图；

图 3 是本发明之远程金融业务系统的本地系统框图；

图 4 是本发明之远程金融业务系统的本地系统框图；

图 5 是本发明之付账模块系统框图；

图 6 是本发明之付账模块初始化流程图；

图 7 是本发明之进行购买业务过程的流程图；

图 8 是图 7 中进行购买业务的处理远程系统中处理步骤流程图。

图 1 所示是本发明之安全在家付账系统。用户操纵付账模块 20，它结合了一个带接收装置的遥控器，该遥控器可用连接方式 30

来完成传送任务，这种连接最好是无线的，可使用任一种无线传送方式，最好使用类似电视红外遥控器，其它如微波、音频或无线电波传送方式也可以。

付账模块和控制装置最好如图 1 所示合为一体，当然在实际中，付账模块既可与其它部件合并，也可以做为独立部分。如果付账模块和其它部件合并，可选择键盘、操纵杆、鼠标或其它控制器来与付账模块进行联络。

在家付账系统其它部分包括直观屏幕 40，如电视屏幕，为存取交互通信网络 80 信息的连接器 50(如图 2 所示)。

直观屏幕 40 有多种，最好是电视，其它如计算机监视器、液晶显示屏等，也可以使用音频连系装置或电话等一些非直观显示器。

具体安装时，连接器 50 可用有线方式和有线电视系统连接。交互通信网络 80 是一个电缆系统；网络连系装置 60 是一个典型的电缆箱，用于和网络 80 联络；连接电缆 50 如图 1 所示连接到电缆箱 60。

交互网络 80 可选择任何类型的网络，只要其能把数据从地方系统 100 传送到远程系统 200，用户能利用其从远程系统 200 接收到数据。另外在电视电缆系统中，所知的交互网络有多种，如 *ATM* 网络、广域计算机网、局部计算机网以及电话线通讯计算机等。安装本发明时，交互网络 80 包括带 *ATM* 网络的有线电视系统。

图 1 的实施例中，付账模块 20 在遥控单元里，由电缆箱 60 来联接，该电缆箱通过连接器 50 输送所需数据到网络 80 中，也能通过网络 80 和连接器 50 从远程系统 200 中接收数据，接收到的数据可同时或分别送到付账模块 20 和显示屏 40。

用户地方系统100经网络80接收从信息源110发来的信息，在具体安装时，网络连系装置接收信息，并经传输线70送到显示屏40，有如电视的天线电缆。这些节目信息可用于多个电视台，并被引导到一种能提供多种物品和服务给用户的在家零售系统。使用时，用户10可从地方系统100所接收到的不同节目中来选择，如同转换有线电视频道，这种选择亦可在计算机控制装置的菜单中进行。

如图3的另一实施例所示，付账模块20与视为遥控单元的控制器22是分开的，付账模块20用有线或无线连接装置32连接到显示屏40、用连接线52和50连接网络。连系装置60有如一个电缆箱，经连线50与网络连接、经连线70与显示屏连接。

图4所示实施例，付账模块和显示屏共同组成付账模块/显示屏组42，这个付账模块/显示屏单元40可直接通过连接器或者如图所示使用连线70、连系装置60和连线50与网络连接。

付账模块20最好是手持式装置，由用户用来输入、发送信号到接收器(如显示屏40或网络连系装置60)。在图5实际装置中，付账模块20包括用户输入装置，如小键盘23。小键盘23最好包含有如电视遥控器的输入键，如数字键0和9、频道控制键、音量控制键等。此外，付账模块可以装有其他输入装置，如光笔、鼠标或触屏等。小键盘23与数据总线25相连，并与付账模块20的其它部件相互作用。数据处理器如微处理器("*MP*")26包括在控制付账模块的功能内。信息和资料存储器28(如可编程只读存储器)存储用户付账账户的数据，也存储付账模块的软件控制程序。可以使用其它类型的存储器如：磁存储器(磁盘驱动器)、先存储器或固态存储器等都很好。这些存储器(如在连系装置、显示屏或在异地的存储器)可以用付账

模块进行遥控。输出适配器29是为付账模块20和接收器之间的远程息通信而提供的。

使用时，付账模块必须用付账账户口令(如"*PINs*")和其它与账户有关的资料来进行初始化。账户可以用多种付账方式，如信用卡、借方卡或支票。同样，最好用存取口令来初始化付账模块，称之为"付账模块口令"。

初始化第一步是用兼密 *DUKPT* 技术的密钥300对付账模块初始化，最好由提供服务者如提供远程金融业务的机构来进行，在此方式中提供服务者保存解密钥或将其提供给相应的用户。

初始化第二步是用用户信息初始化付账模块，这一步最好由用户使用图5所示的付账模块来执行。用户可用小键盘23输入信息，并存储在付账模块里，例如信息和资料存储器28。指令、菜单和提示由付账模块提供给显示屏40(如使用输出29)。

图6实施例中，付账模块是用步骤310中与第一信用卡对应的信息来初始化，典型的，在该信用卡初始化步骤310中输入的信息与磁道1或磁道2卡片数据相对应，通常磁道1或磁道2数据在借方卡或信用卡的磁条上进行编码，要求磁条阅读器能获得磁条之外的信息，使用时，用户可通过阅读器获得数据。磁道1数据典型地对应于持卡人姓名、账号、截止日期以及卡验证值("*CVV*")或 *PIN* 验证值("*PVV*")。*CVV* 和 *PVV* 用于 使用已有技术对其它信息的检验，通常它们是与磁条的其它数据相对应的数据值，由卡片发行人制定。磁道2的数据与磁道1相同，但不包括持卡人姓名。

进入步骤310的用户信息应与磁道1或磁道2数据或以上两者或某些其它信息集合相对应，由用户把信息输入付账模块。最好，卡

片发行人给用户 10 一串字符，用户可将其输入付账模块中。数字串与 步骤 310 的输入用户信息相对应。在最佳实施例中，由付账模块 20 把信号输送给显示屏 40，用户在图示菜单和提示下，一步接一步按处理程序输入数据，输入数据后，接着运行检验程序 320。典型的检验程序使用已知的逻辑冗余检验技术，用户输入自己的字符，便于检验所输用户信息是否正确。如果检测到有错误，付账模块则要求执行步骤 330 进行数据改正，如检测无误则继续下一步。

下一步骤 340。用户在提示下利用已初始化的卡片输入加密 *PIN*，加密 *PIN* 由步骤 345 提供。在最佳实施例中，提供一个如上述的文件加密器给用户，产生一个加密 *PIN*；并使用由卡片发行人掌握的密钥，密钥在付账模块中取不到，这样恶意进入付账模块者无法拿得到。加密 *PIN* 由用户输入付账模块，也可以直接给显示屏 40 指令，把加密 *PIN* 存储在付账模块中。

步骤 350，系统对是否初始化附加卡片进行询问。如果有附加卡片则接着运行下一步步骤 360，并运行 310—350 步对附加卡片进行初始化；如果没有附加卡片，继续进行初始化步骤的最后一步。

最后是步骤 370。用户在提示下选择付账模块口令，该密码用来控制进入付账模块。付账模块口令被输入付账模块里并被保存在如程序和信息存储器 28。付账模块最好不需输入密码即可用作显示屏 40 或接口/电缆箱 60 的遥控器；同样道理，用输入付账模块口令应能起到限制付账功能，此外付账模块口令应能进入定购或付账系统，因此，用户的付账账户和加密 *PINs* 仅仅为该用户使用。

在另一实施例中付账模块口令和付账账户信息可由多个用户输入，用 不同的密码来处理不同的账户。

在另一实施例中，也可以由处理中心如银行用付账账户信息初始化付账模块，这个实施例中的处理中心有一个磁条阅读器与付账模块相连，可把数据传送给模块，这样磁条阅读器可以补充或取代当做输入器的小键盘 23 来进行初始化。操作者将选择的卡划过阅读器，这种划卡过程使磁条阅读器获取需要的磁条上的信息，如磁道 1 和磁道 2 的信息。磁条阅读器自动把需要的信息输出到付账模块中，再由付账模块用上述方法进行存储。另外，用户还可以把需要的 *PINs* 输入磁条阅读器(就象使用一个联机小键盘，磁条阅读器，对输入的 *PINs* 进行加密，加密后的 *PINs* 被送往付账模块进行存储。

操作中，各种金融业务均可使用付账模块进行处理，图 7 是一种典型的处理系统，用户可以使用该系统进行购物或获得服务，也可用于电子资金转账，如不同账户间的付账和转账。

这些业务系统的共同特点是：能自动提供账户信息(如磁道 1 或磁道 2 信息)；并由付账模块加密 *PINs*，用户除付账模块口令外无需输入其它信息或未加密 *PINs*，即可使用该金融业务系统，这些密码数字/*PINs* 用户必须记住。

运行时，显示屏 40 能按顺序显示交互的提示，指导使用购买业务，提示最好是由付账模块 20 来提供，也可以通过网络从远地点获得。通常的业务中，用户可以依步骤 400 的提示，输入它的付账模块口令，也可直接使用提示和菜单选择特定的业务。

购物时，需要的项目是指定的。例如：用户指定所需商品或服务为 410(如输入产品代码)、所需数量为 420，接着在提示下核实所购物品的金额 430，如果用户对此金额有异议则返回步骤 410 重新进

行选择。

金额核实无误后，用户接着选择付款方法 440，付款方法是被用于初始化付账模块的付款账户之一，例如，用户可以选择付账模块已初始化的信用卡或借方卡，并通过显示屏 40 显示的菜单使用小键盘 23 选择付款账户。

步骤 450。为更加安全可靠，付账模块根据已选择的付款方式对上述已加密的 *PIN* 进行再加密，加密步骤 450 可使用任一种加密技术，但最好使用 *DUKPT* 技术。同样，所需账户资料可在步骤 450 加密，该账户资料可以与磁道 1、磁道 2 或其它需要的账户的资料一致。

双加密 *PIN* 和加密账户资料如步骤 460 所示被输送到交互网络 80。

交互网络最好和处理机构 90 如银行办理机构相联络，大多数处理机构都可以与网络相连接，这样，用户或团体利用在家购物系统在处理机构中选择所需物品。

步骤 500 中处理机构 90 通过网络 80 接收加密 *PIN* 和账户资料，可以如步骤 510 所介绍的利用账户资料鉴别付款账户。一般情况下，处理机构 90 在数据处理系统接收加密 *PIN* 和账户资料，数据处理系统对加密账户资料进行解密，根据解密后账户资料，数据处理系统识别付账账号和识别机构 95 管理的账户，如步骤 520 所述的相关银行或金融机构。通常该机构所保存的账户可从账号上识别，因为账号一般包含各个发行机构所特有的识别码。

处理机构经网络 80 把加密 *PIN* 和账户资料（加密或不加密）传送给付款账户机构 95，如果需要，付款账户机构可依步骤 530，把

加密 *PIN* 和账户资料进行解密。通常，付款账户机构 95 在数据处理系统接收这些数据，数据处理系统将加密账户资料进行解密。如步骤 540 所述，账号和 *PIN* 最好经过识别，然后由付款账户机构 95 决定接受或拒绝该业务，例如，该机构可通过检查现有账号的数据库来识别账号；该机构还可以这样识别 *PIN*：确认该 *PIN* 是否与指定给该账号的 *PIN* 一致。对于决定接受还是拒绝一项业务比如购物活动，该机构可以把购物所需金额同账户上的信用卡限额进行核查对照；如果购物金额超出了信用卡限额，一般来说该项业务将被拒绝。

一旦付款账户机构 95 决定接受/拒绝该项业务后，一个接受/拒绝信息经网络 80 送回到本地系统。

由上述可见，一种远程金融业务系统被提供出来。熟练掌握本技术的人将会认识到本发明的实用性不限于实施例，实施例仅是示例，不作限定。本发明由权利要求书来限定。

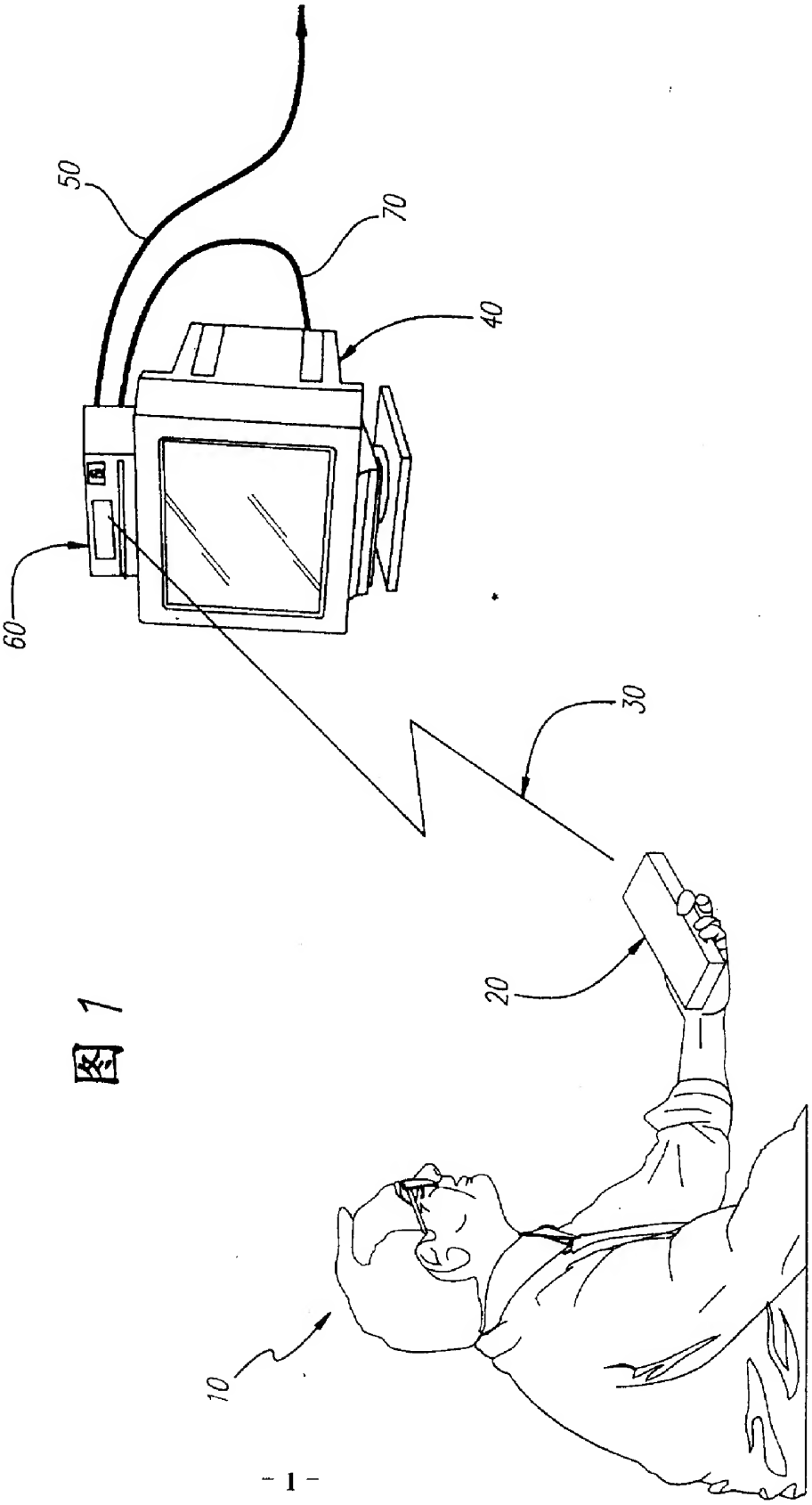


图 1

图2

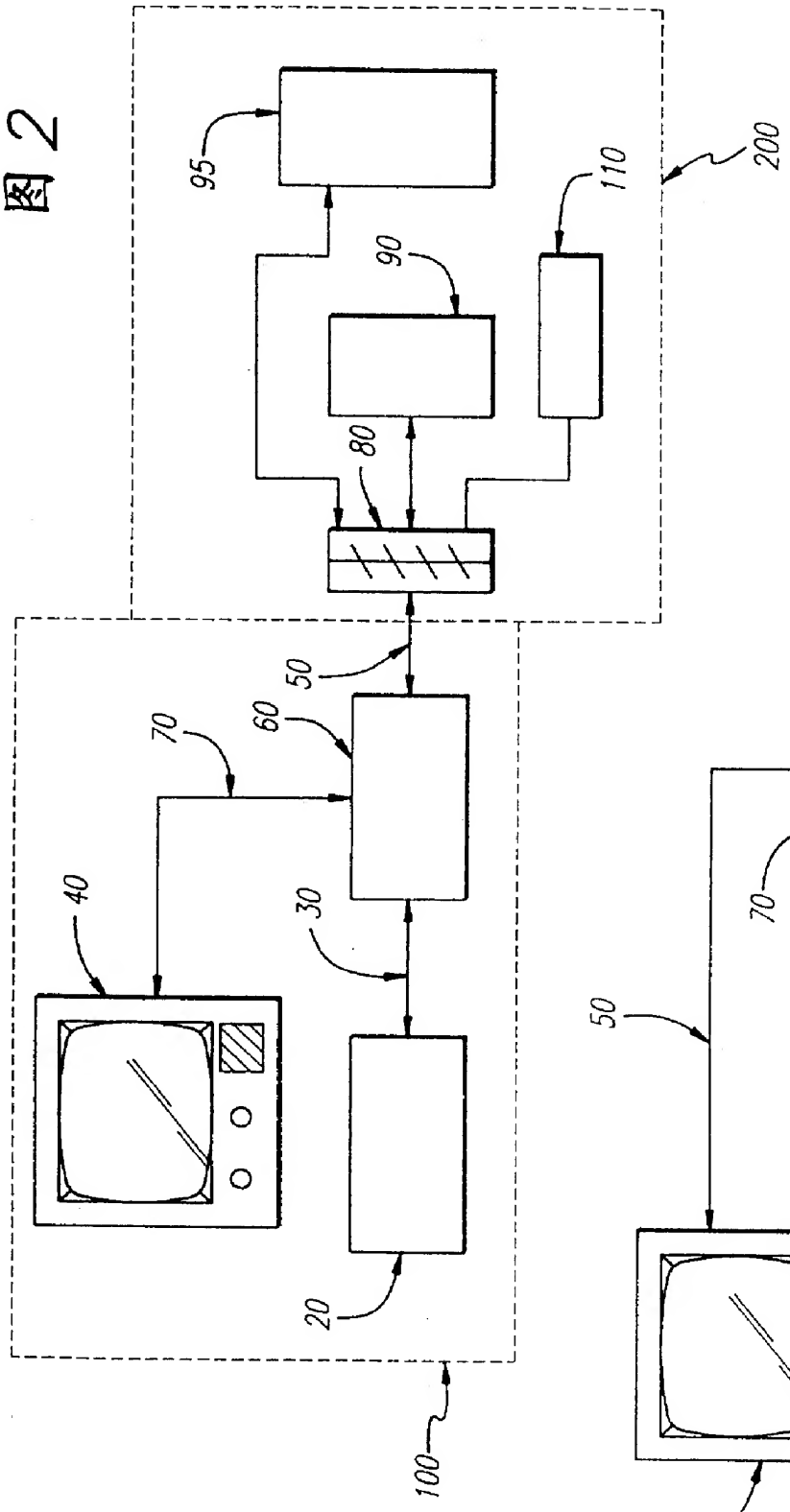


图3

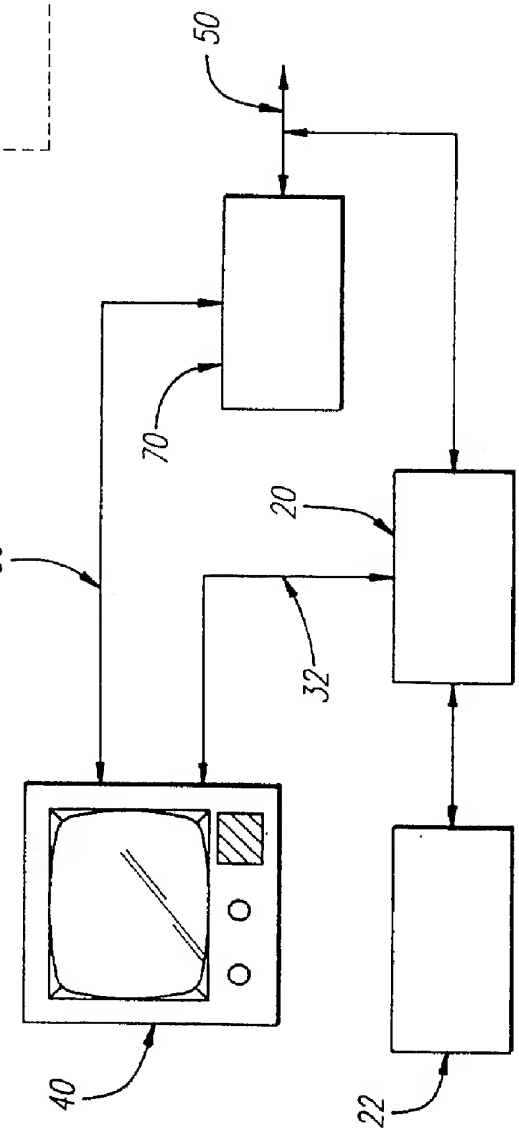
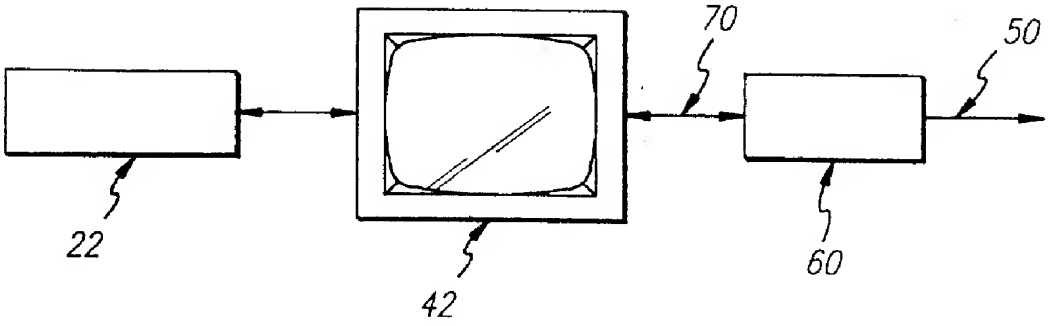


图 4



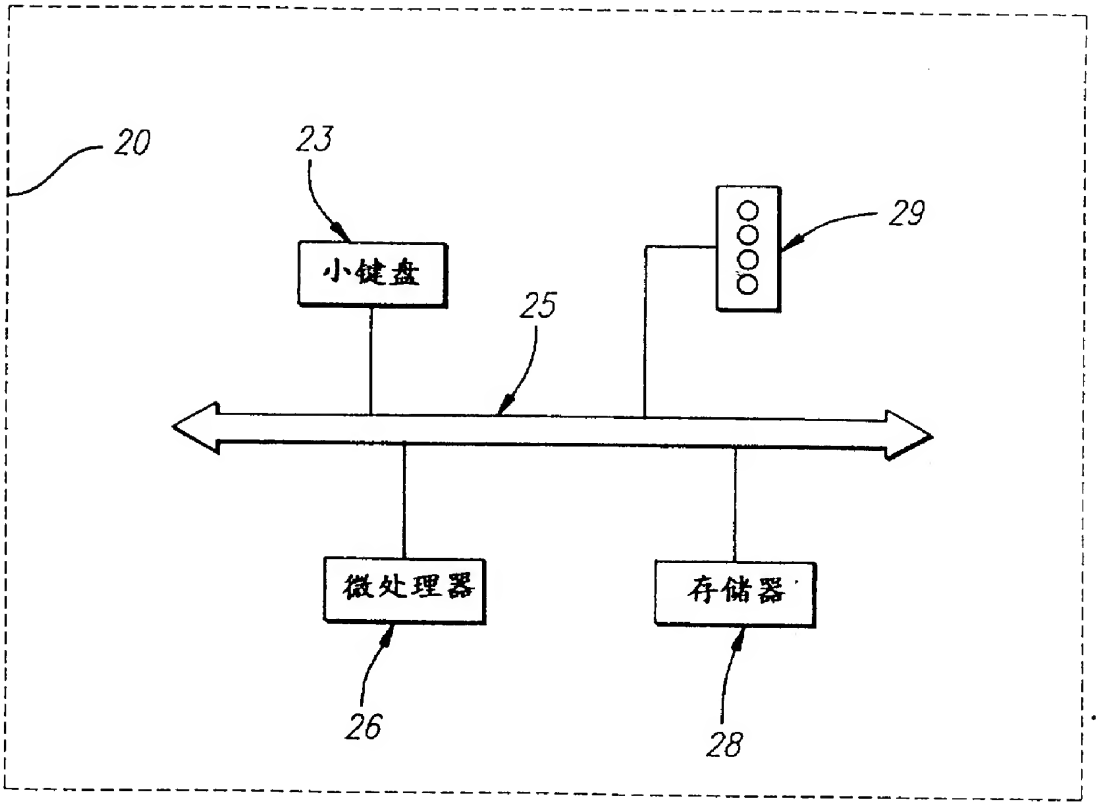


图 5

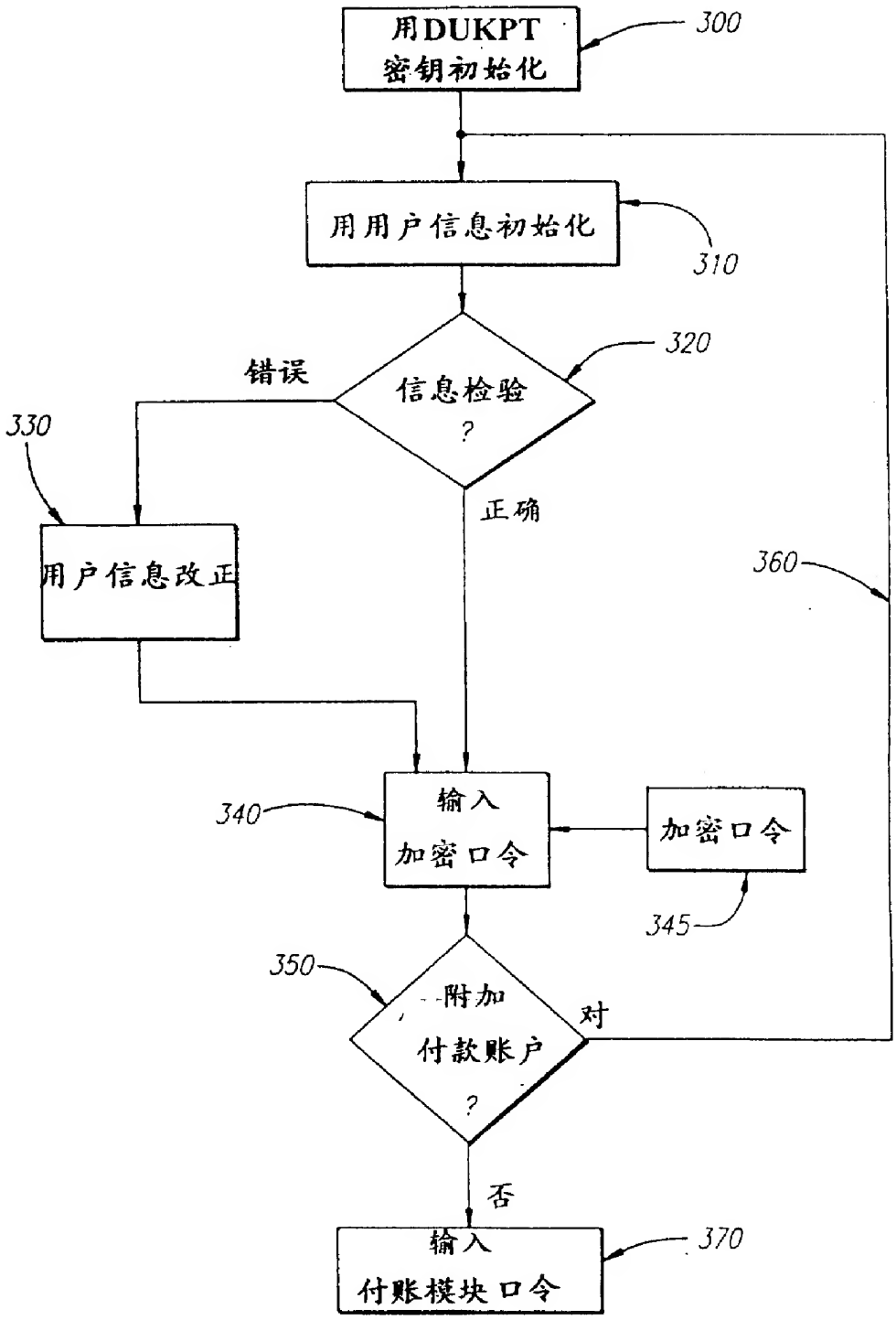

用DUKPT
密钥初始化
300
用用户信息初始化
310
信息检验
?
320
错误
330
正确
用户信息改正
360
输入
加密口令
340
加密口令
345
附加
付款账户
?
350
对
否
输入
付账模块口令
370

图 6

图 7

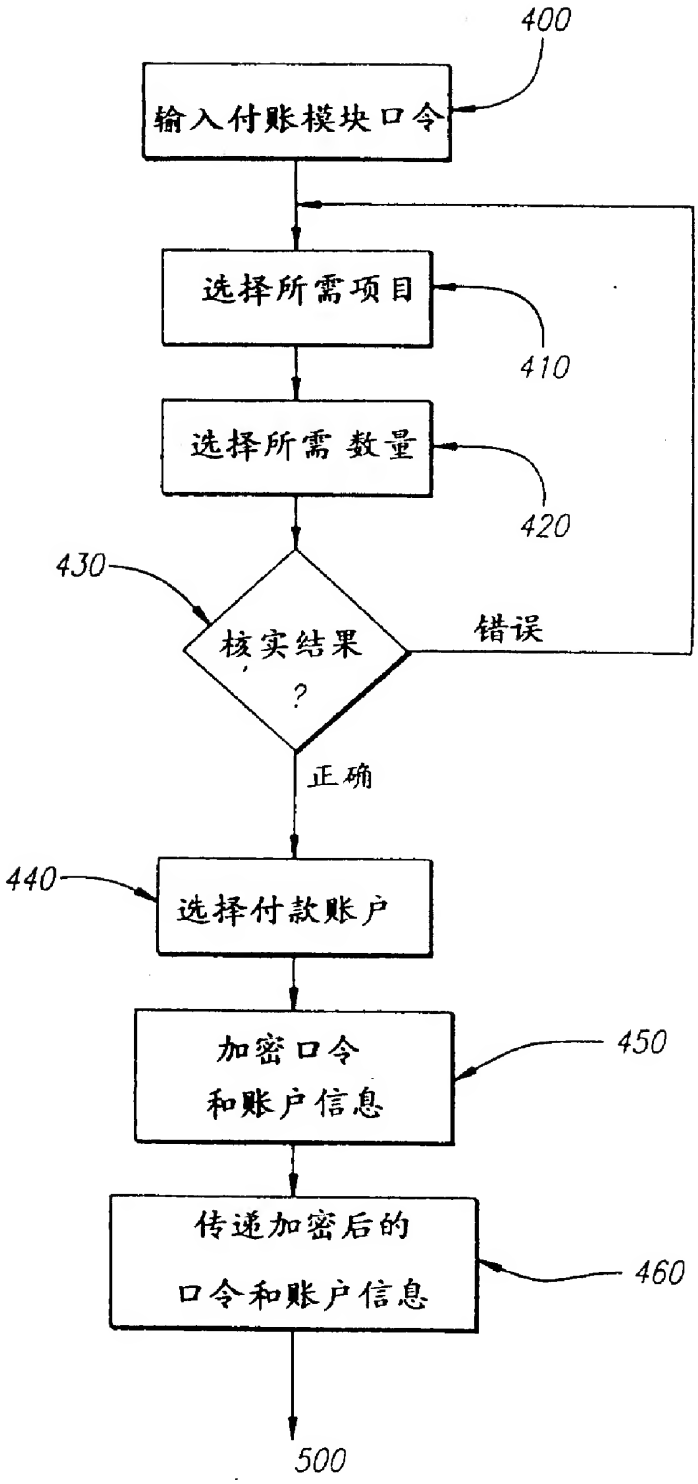
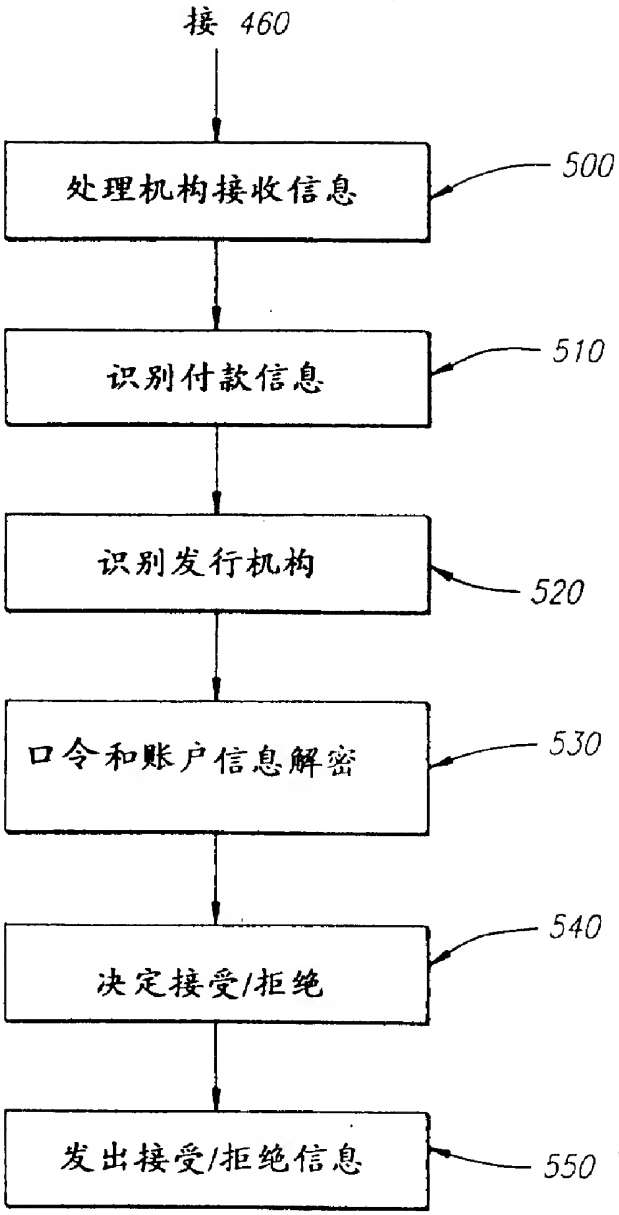

400
输入付账模块口令
选择所需项目
410
选择所需 数量
420
430
核实结果
?
错误
正确
440
选择付款账户
加密口令
和账户信息
450
传递加密后的
口令和账户信息
460
500

图 8


接 460
处理机构接收信息
500
识别付款信息
510
识别发行机构
520
口令和账户信息解密
530
决定接受/拒绝
540
发出接受/拒绝信息
550